MAYER BROWN LLP
Lauren R. Goldman (*pro hac vice*)
Michael Rayfield (*pro hac vice*)
1221 Avenue of the Americas
New York, NY 10016
(212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

Matthew D. Provance (*pro hac vice*)
71 Wacker Drive
Chicago, IL 60606
(312) 701-8598
mprovance@mayerbrown.com

COOLEY LLP
Michael G. Rhodes (116127)
Whitty Somvichian (194463)
101 California Street, 5th Floor
San Francisco, CA 94111
(415) 693-2000
rhodesmg@cooley.com
wsomvichian@cooley.com

Attorneys for Defendant Facebook, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CLAYTON P. ZELLMER,

Plaintiff,

vs.

FACEBOOK, INC.,

Defendant.

Case No. 3:18-cv-1880-JD

DEFENDANT'S REPLY IN SUPPORT OF SUMMARY JUDGMENT

Date: July 8, 2021
Time: 10:00 a.m.
Location: Courtroom 11, 19th Floor
Judge: Hon. James Donato
Trial Date: April 11, 2022
Complaint Filed: March 27, 2018

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION[1]

Mr. Zellmer's opposition does not even mention the central allegations on which he based this suit—that Facebook created and stored a template based on a photo of his face, compared it to subsequent photos of his face, and identified him by name. Compl. (Dkt. 1) ¶¶ 22, 24, 35-36. He understands that his allegations were false: Facebook has never created or stored a template for Mr. Zellmer, a non-user, or otherwise identified him through the use of facial recognition. McCoy Decl. (Dkt. 66-11) ¶ 15.

Mr. Zellmer is therefore left to argue that ephemeral *face signatures*—temporarily created from images of non-users as an intermediate step in Facebook's facial recognition process for *consenting users*—are "biometric identifiers" under BIPA. 740 ILCS 14/10.[2] But discovery has disproven that contention as well: Non-user face signatures are not "biometric identifiers" (or otherwise covered under BIPA) because they are not—and cannot be—used to identify anyone; [redacted]; and they are not the type of data the legislature intended BIPA to cover. McCoy Decl. ¶¶ 15-16.

Mr. Zellmer characterizes these arguments as "fact-specific" and asserts that "a reasonable jury" could resolve them in his favor. Opp. 9. However, he makes no attempt to rebut any of the facts material to those arguments. Mr. Zellmer does attempt to muddy the waters by littering his brief with irrelevant (and often false) allegations about Facebook's data practices in general. But his brief confirms that the three grounds for summary judgment advanced by Facebook raise no disputed issues of material fact and present purely legal questions for this Court. And when it comes to the law, Mr. Zellmer is wrong.

First, Mr. Zellmer argues that face signatures qualify as "biometric identifiers" under BIPA even though they cannot be used to identify an individual. He contends that Facebook's contrary

---

[1] "MSJ" refers to Facebook's motion. "Opp." refers to plaintiff's opposition. "Ex. __" refers to exhibits to the Declaration of Matthew D. Provance, filed with Facebook's motion. "Milian Ex. __" refers to exhibits to the Declaration of David P. Milian, filed with plaintiff's opposition. All emphases are added unless otherwise noted.

[2] Mr. Zellmer has abandoned any claim that Facebook collected his "biometric information," the only other category of data regulated under BIPA. *See* Opp. 10.

argument "improperly conflates" the definition of "biometric identifier" with the definition of "biometric information"—which is expressly limited to data that is "used to identify an individual"—and that the terms should be treated differently under "canons of statutory construction." Opp. 11. But there is an obvious reason why the "used to identify" language appears in only one of the two definitions: There was no need for the term "biometric identifier" to include a similar express limitation because the word "identifier" is right there *in the term itself*. That limitation is not self-evident for biometric information—data "based on" a biometric identifier—so the legislature had to make clear that such derivative data is "*still* covered by [BIPA] *if* that information can be *used to identify the person*." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017). In effect, Mr. Zellmer asks the Court to read the word "identifier" out of the statute.

Second, Mr. Zellmer argues that even though face signatures [redacted], Facebook "possess[es]," "collect[s], capture[s], . . . or otherwise obtain[s]" them under BIPA. 740 ILCS 14/15(a), (b). He relies on the fact that the data is "create[d] and compare[d]" (unsuccessfully) to user templates. Opp. 16. But courts construing the relevant terms have held that the statute applies only when an entity "h[olds] the data at its disposal" or can otherwise "freely access" it. *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020). Only an entity with that "dominion or control" over data can use it to identify someone in the future, invade her privacy, or steal her identity. *Id.* Mr. Zellmer does not explain how Facebook can use ephemeral data for these purposes. While he attempts to distinguish Facebook's authorities, he cites none of his own.

Third, Mr. Zellmer argues that even though Facebook could not possibly obtain consent from non-users, applying BIPA to face signatures would not force Facebook to shut down facial recognition because the statute penalizes only negligent, reckless, or intentional violations; he asserts that Facebook could therefore escape liability by showing that it made "reasonable" *efforts* to comply. Opp. 7-8. Mr. Zellmer misunderstands BIPA. Although he correctly points out that Facebook cannot be held liable for *damages* unless he carries his burden of proving (at least) negligence, BIPA's requirements are mandatory: "Any person aggrieved" by any violation has a

right of action to pursue various forms of relief, both monetary and equitable—regardless of the defendant's scienter or lack thereof. 740 ILCS 14/20. Mr. Zellmer's reading of BIPA would effectively ban Facebook's technology, along with others that the legislature specifically expressed a desire to *promote*, by making it impossible to avoid liability as to non-users.

For these reasons, Facebook is entitled to summary judgment on each of Mr. Zellmer's claims. But in any event, Mr. Zellmer's request for an injunction "requiring Facebook to comply" with BIPA must be dismissed. Compl. ¶ 56. Again, Mr. Zellmer suggests that such an injunction would be permissible because it would merely force Facebook to show that it *tried* to comply with BIPA. And again, that is not how BIPA works. Mr. Zellmer's injunction would necessarily force Facebook to shut down facial recognition altogether. Because this would harm numerous "individuals who are not members of the putative class"—including consenting users who *want* the feature—he cannot obtain that relief. *Stokes v. CitiMortgage, Inc.*, 2015 WL 709201, at *10 (C.D. Cal. Jan. 16, 2015).

This is not the *Facebook Biometric* action, which was based on the creation and storage of face templates to identify users. Mr. Zellmer cannot shoehorn non-user face signatures into BIPA's clear regulatory scheme.[3]

I. THE DATA DERIVED FROM MR. ZELLMER'S PHOTOS IS NOT A "BIOMETRIC IDENTIFIER" BECAUSE IT CANNOT BE USED TO IDENTIFY HIM.

A. There Is No Genuine Dispute That Facebook Cannot Use Facial-Recognition Data To Identify Non-Users Like Mr. Zellmer.

Mr. Zellmer concedes that face signatures temporarily created from images of non-users cannot be used to identify anyone. Opp. 9-14.[4] Because he has abandoned any contention that

---

[3] Mr. Zellmer repeatedly asserts that Facebook has not sought judgment on his claim under Section 15(a) of BIPA. Opp. 8, 17 n.52. That is wrong. Facebook has moved for summary judgment on "all of plaintiff's claims" (MSJ at 21), and Facebook's arguments go to whether it has obtained his "biometric identifier" (a requirement for all of Section 15's provisions); whether Facebook "possess[ed]" his biometric data (a requirement specific to Section 15(a)); and whether Mr. Zellmer's reading more generally would violate Illinois law.

[4] Mr. Zellmer does note that Facebook's system erroneously matched his face to a *user's* profile. Opp. 6. [redacted]. MSJ 6 n.5. [redacted]

templates are created for non-users, and limited his claim to whether face signatures are "biometric identifiers" under BIPA (Opp. 10), this concession should end the case. As discussed below, the term "biometric identifier" encompasses only data that that is used to identify an individual.[5]

Mr. Zellmer briefly claims that certain metadata allegedly collected from images of non-users—the location of the face box within the image and [redacted]—"can identify an individual." Opp. 14. This assertion is both wrong and irrelevant for at least three reasons. First, Mr. Zellmer does not (because he cannot, *see* McCoy Decl. ¶ 16) even claim that this information can be used to identify *the non-user* who appears in the photo; his assertion is that the data is associated with *the account of the user who uploaded* the photo. Opp. 14. Second, he provides *no evidence* that the mere position of a face in a photo could ever be used to perform an automated identification of anyone. Third, BIPA expressly exempts "demographic data" [redacted] from its coverage. 740 ILCS 14/10. That makes sense: demographic data does not identify individuals; it classifies them into large groups such as "male" or "18-24." Mr. Zellmer appears to concede these points: he refers to this information as "biometric data" (Opp. 14), but stops short of asserting that it constitutes a "biometric *identifier*."[6]

B. BIPA Regulates Only Data That Is Used For Identification.

Facebook's motion set forth several reasons why it is clear from the face of BIPA that the term "biometric identifier" covers only data used to identify an individual. MSJ 12-15. Mr. Zellmer ignores most of these reasons, and his limited responses are meritless.

1. Mr. Zellmer Ignores The Plain Meaning Of "Biometric Identifier."

Although Mr. Zellmer acknowledges that statutory interpretation begins with the plain meaning of the terms (Opp. 11), he ignores what is plain in the term "biometric *identifier*":

[redacted]. *Id.*; McCoy Decl. ¶ 15.

[5] Because this is obviously what Facebook argued in its motion (MSJ 13), Mr. Zellmer's assertion that Facebook's "MSJ does not contest that a face signature is a 'biometric identifier'" (Opp. 10) is baffling.

[6] Mr. Zellmer also asserts that his face was tagged by name in a photo uploaded to Facebook. Opp. 6. Not so. The user who uploaded the photo (of two individuals), simply wrote a caption that included a reference to "Clyde Zellmer." Milian Ex. 14 at ZELLMER00011. This fact only underscores that *Facebook* cannot identify non-users who appear in uploaded photos.

"Identifier" *means* "one that identifies," and "identify" means "[t]o establish the identity of." WEBSTER'S DICTIONARY (2008 ed.) (EX. 7). Accordingly, both the courts and the Illinois Attorney General have recognized that the term "biometric identifier" encompasses only biometric data "that can be *used to identify a person*." *Rivera*, 238 F. Supp. 3d at 1094; *see* Public Access Op. No. 17-011, 2017 WL 10084298, at *3 (Ill. A.G. Aug. 14, 2017) (construing the term to mean data "*that identifies a person*").[7]

Mr. Zellmer urges the Court to disregard the Attorney General's construction because it was interpreting the term "biometric identifier" in Illinois' Freedom of Information Act. Opp. 13. But of course, statutory terms are never interpreted in a vacuum; they are given their "commonly understood" meaning. *See King v. Illinois Indus. Comm'n*, 301 Ill. App. 3d 958, 962 (1998). And Mr. Zellmer overlooks that the Attorney General expressly noted that its construction was consistent with how the term "biometric identifier" is "commonly used in Illinois law," *including in "[t]he Biometric Information Privacy Act*." Public Access Op. No. 14-008, 2014 WL 4407615, at *2 (Ill. A.G. Aug. 19, 2014). In any event, Mr. Zellmer makes no attempt to address what dictionaries make clear, or the court's decision in *Rivera*, which unambiguously construed BIPA.

2. Mr. Zellmer Cannot Avoid The Meaning Of "Biometric Identifier" By Arguing That The Data At Issue Is A "Scan Of Face Geometry."

Mr. Zellmer ignores the plain meaning of "biometric identifier" and argues that data is regulated by BIPA so long as it fits within the meaning of the items listed in the definition of that term, including "scan of . . . face geometry." Opp. 12. He is wrong.[8]

---

[7] *See also* Jane Illman, *Data Privacy Laws Targeting Biometric and Geolocation Technologies*, 73 Bus. Law. 191-92 (2018) ("[B]iometric identifier, . . . as the name implies, is data associated with a person's biological marker that can later be *used to identify that specific individual*.").

[8] Mr. Zellmer makes another disingenuous attempt to claim an easy victory, asserting that Facebook has "concede[d]" that face signatures are "scans of . . . face geometry" under BIPA. Opp. 10. Mr. Zellmer points (Opp. 10 n.40) to language in Facebook's motion *expressly disclaiming* any such concession (MSJ 11 n.6). To clarify, at this stage, Facebook is not raising arguments *specific* to the term "scan of face geometry," such as whether its technology relies on the relationships between human-notable facial features. *Cf.* Dkt. 298-24 at 19-23, *In re Facebook Biometric Privacy Litig.*, No. 15-cv-3747 (N.D. Cal.). Facebook is making a more straightforward argument at summary judgment: that a face signature does not qualify as *any* kind of "biometric identifier" because it cannot be used to identify an individual.

As the *Rivera* court explained, the definition simply "specifies each particular *type* of covered biometric identifier." 238 F. Supp. 3d at 1094. "Each specific item on the list," including "scans of face geometry," still must "fit[] within the meaning of the term 'biometric identifier,' that is, a biology-based set of measurements ('biometric') that can be *used to identify a person ('identifier.')*." *Id*. In other words, the scope of each item listed in the definition is informed and limited by "the ordinary meaning of [the] defined term, particularly [to the extent] there is dissonance between that ordinary meaning and the reach of the definition." *Bond v. United States*, 572 U.S. 844, 861-62 (2014) (applying "[t]he ordinary meaning of 'chemical weapon'" even though it was defined in the statute).

In any event, even if one were to focus exclusively on the listed items, the outcome would not change. For example, the definition of "biometric identifier" includes a "fingerprint," which is defined as "an ink impression of the lines upon the fingertip taken *for the purpose of identification*" (MERRIAM-WEBSTER.COM, https://www.merriam-webster.com), and a "voiceprint," which is defined as "[a] distinctive pattern of curved lines and whorls made by a machine that measures human vocal sounds *for the purpose of identifying an individual speaker*" (BLACK'S LAW DICTIONARY). The other listed items, including "scan of face geometry," must be interpreted according to the "general rule that words grouped in a list should be given related meaning." *Dynak v. Bd. of Educ. of Wood Dale Sch. Dist. 7*, 2020 IL 125062, ¶ 22 (2020). The meaning that unifies the terms—particularly given that they all constitute types of "biometric *identifiers*"—is that they are used to identify.

3. The Definition Of "Biometric Information" Does Not Help Mr. Zellmer.

Mr. Zellmer argues that because BIPA's term "biometric information" is expressly limited to data "used to identify an individual," no such limitation can be read into the definition of the term "biometric identifier." Opp. 11. This argument is irreconcilable with the text, purpose, and structure of the statute. *See People v. Zimmerman*, 239 Ill. 2d 491, 497 (2010).

Text. The limitation to data that is used to identify is inherent in the plain meaning of the term "biometric identifier." Additional qualifying language in the definition of that term (*e.g.*,

defining a "biometric *identifier*" as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry *used to identify* an individual") would have been utterly superfluous.

Purpose. The purpose of BIPA, as explained in its legislative findings, is to regulate "biologically unique" "*identifiers*." 740 ILCS 14/5(c). The legislature could have sought to regulate mere "biometric *data*"—"a biology-based set of measurements," *Rivera*, 238 F. Supp. 3d at 1094[9]—but it chose not to do so because it was specifically concerned with data that could be "used to access finances or other sensitive information," and to commit "identity theft." 740 ILCS 14/5(c). These and similar invasions of privacy can be accomplished only with data that identifies a specific person. Thus, the legislature enacted regulations that would permit people to comfortably "partak[e] in biometric *identifier*-facilitated transactions." *Id.* 14/5(e). Mr. Zellmer does not address *any* of these express legislative findings.

Structure. The structure and legislative history of BIPA confirm this point. The General Assembly decided to regulate a category of derivative data that it called "biometric information"—data "based on an individual's biometric identifier" (740 ILCS 14/10)—because it recognized that a private entity could potentially "evade . . . the Act's restrictions by converting a person's biometric identifier into some other piece of information." *Rivera*, 238 F. Supp. 3d at 1095. Its goal was to ensure that "whatever a private entity does in manipulating a biometric identifier . . . , the resulting information is *still* covered by [BIPA] if that information can be *used to identify the person*." *Id.* The "used to identify" language was simply necessary to clarify what "biometric information" is. Eliminating any doubt, the statute expressly describes *both* "biometric identifiers" *and* "biometric information" as forms of "confidential and sensitive information" (740 ILCS 14/15(e)(2)), defined to mean "information that can be *used to uniquely identify an individual* or an individual's account or property" (*id.* 14/10).

---

[9] *But see* CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/ (defining "biometric" as "information about someone's body, such as the patterns of color in their eyes, that can be *used to prove who that person is*"); MERRIAM-WEBSTER.COM, https://www.merriam-webster.com (defining "biometrics" as "the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially *as a means of verifying personal identity*").

Mr. Zellmer's reading also makes no sense. "Biometric identifiers" and "biometric information" are regulated the exact same way. *Id.* 14/15. There is no reason why the legislature would want to regulate *original* data that *cannot* identify someone, while also regulating *derivative* data only if it *can* be used to identify someone. The entire point of creating the "biometric information" category was to prevent a private entity from manipulating an original source of biometric data in a way that would still enable the entity to identify someone—outside the purview of the statute.

4. The Cases Confirm That Data Qualifies As A "Biometric Identifier" Only If It Can Identify An Individual.

Facebook cited several cases, in addition to *Rivera*, that confirm its reading of "biometric identifier." MSJ 13-15. Mr. Zellmer makes a weak attempt to distinguish some—but not all—of those cases. Opp. 13-14. For example, he dismisses the Ninth Circuit's opinion in *Patel v. Facebook, Inc*., 932 F.3d 1264 (9th Cir. 2019), because it addressed Article III standing rather than the substance of a BIPA claim. Facebook acknowledged as much (MSJ 13), but Mr. Zellmer misses the point: The court's finding on standing was based on its recognition that the "substantive harm targeted by BIPA" was the "alleged collection, use, and storage of plaintiffs' *face templates*," which "Facebook can use [ ] *to identify [an] individual*" in subsequent photos. *Id.* at 1273, 1275.

The only case Mr. Zellmer affirmatively *relies* on is *Hazlitt v. Apple, Inc.*, 500 F. Supp. 3d 738 (S.D. Ill. 2020)—which Facebook addressed in its motion. MSJ 14-15. But Mr. Zellmer mischaracterizes that decision. The Apple feature at issue allegedly created "facial *templates*" from photos and stored them in a database so that Apple could recognize the same face in subsequent photos and group them together. *Id.* at 742, 748; *see also* Dkt. 1-1 ¶ 74, No. 3:20-cv-421 (S.D. Ill. 2020). Apple argued that it was not using the templates to "*actually* identify any individual" and that they "do not qualify as biometric identifiers . . . *because they are anonymous*." 500 F. Supp. 3d at 748. *That* is the reading of BIPA that the court deemed "too narrow." *Id.*

That it is not the argument that Facebook is making here: Face signatures generated from images of non-users *cannot* be used to identify anyone—not only because they are not associated with any name, but because, among other reasons, they are [redacted] rather than

converted into a stored template that can ever be used to generate a match. There is no genuine dispute on this point.

Indeed, *Hazlitt* confirms *Facebook's* position that only data that *can* be used to identify a person qualifies as a "biometric identifier." In the sentence that immediately follows Mr. Zellmer's block quote (Opp. 14), the court explained: "Each specific item [in the definition of 'biometric identifier'] fits within the meaning of [that] term . . . . The word 'identifier' modifies the word 'biometric' to signal that the types of data listed *could* be used to identify a person." *Hazlitt*, 500 F. Supp. 3d at 749 (emphasis in original). Mr. Zellmer's reliance on a cherry-picked quote from *Hazlitt* does not help his argument.

In sum, because non-user face signatures are not and cannot be used to identify anyone, they are not "scans of face geometry" or any other type of "biometric identifier" under BIPA.

II. FACEBOOK WAS NEVER IN "POSSESSION" OF MR. ZELLMER'S ALLEGED "BIOMETRIC IDENTIFIERS" AND DID NOT "COLLECT," "CAPTURE," "OR OTHERWISE OBTAIN" THEM.

BIPA does not apply to face signatures because Facebook does not "possess[]," "collect, capture, . . . or otherwise obtain" them. MSJ 15-18; 740 ILCS 14/15(a)-(b). In order to do any of these things, an entity must "h[old] the data at its disposal" or otherwise be able to "freely access" it. *Heard*, 440 F. Supp. 3d at 968 (quotation marks omitted). There is no genuine dispute that Facebook does not exercise this "dominion or control" over face signatures (*id.*)—[redacted] (McCoy Decl. ¶¶ 8, 11, 16). Mr. Zellmer notes that the plaintiffs' expert in *Facebook Biometric* testified that "there is a notion of storing a face signature, but that is a temporary storage." Opp. 15. Facebook disagrees with the expert's description, but it makes no difference to the *legal* question of whether face signatures are "posses[ed]" or "obtained" under BIPA: Mr. Zellmer does not dispute that [redacted]. *Compare* MSJ 15 *with* Opp. 14-15.

Mr. Zellmer insists that Facebook's "control over the data is so complete that [the data does] not even exist until Facebook create[s]" it. Opp. 17. The problem with this argument is that the word "create" is nowhere in the statute. And the terms BIPA *actually* uses have been interpreted in a manner that cannot possibly apply to the mere creation of data that exists only

ephemerally. *See Heard*, 440 F. Supp. 3d at 968; *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279, 283-84 (N.D. Ill. 2019). This makes sense: Facebook cannot use data that exists only ephemerally to identify someone (the conduct BIPA regulates) or to steal their identity or otherwise invade their privacy (the harm BIPA seeks to prevent). MSJ 16; 740 ILCS 14/5(c). Mr. Zellmer dismisses these cases as "inapposite" (Opp. 16), but they construed the very terms at issue in light of Illinois Supreme Court precedent. And he cites *no* cases in support of his interpretation.

Mr. Zellmer therefore falls back on the argument that BIPA should be read to apply to the mere creation of face signatures because Facebook has not proven that a hacker could *not* "intercept" one and use it to commit identity theft. Opp. 15. That is wrong. Facebook offered undisputed evidence that [redacted]. MSJ 5-6, 15; McCoy Decl. ¶¶ 7, 12. So even if a hacker were to somehow "intercept" one [redacted], there would be no risk of identity theft [redacted]. McCoy Decl. ¶ 12. In any event, Mr. Zellmer has the burden of proof, and he has offered no evidence that face signatures *can* be "intercepted" and used to commit identity theft. Indeed, by asserting that "[t]he advances in technological tools available to hackers and their sophistication level continue to grow exponentially" (Opp. 15-16), he implicitly admits that he cannot prove the speculative claim in his brief. More fundamentally, though, Mr. Zellmer has not shown that *Facebook*—as opposed to a hypothetical hacker—retains any control over the data at issue. His claims therefore fail.

III. BIPA DOES NOT APPLY TO THE DATA AT ISSUE BECAUSE THE STATUTE DOES NOT REQUIRE IMPOSSIBLE NOTICE AND CONSENT.

The General Assembly plainly did not intend for BIPA to forbid the incidental analysis of non-user photos that is necessary for a facial-recognition system to function for consenting users. Because it would be impossible to obtain informed consent from non-users, applying BIPA in this situation would effectively ban the technology, contrary to the legislature's clear intent. *See* MSJ 19; 740 ILCS 14/5(a), (e), (g). Mr. Zellmer's lawyers have had five years to address this fundamental defect in their claim, after the Court repeatedly told them in *Gullen* that it would be

"patently unreasonable" to interpret "a written consent statute" in a way that would amount to a "ban [o]n the program." Ex. 5 at 9-10. The best answer they can come up with is that their reading would not amount to a ban because BIPA does not actually *require* "100%" compliance. Opp. 8. That is as wrong as it sounds.

Mr. Zellmer starts from the premise that BIPA penalizes only negligent, reckless, or intentional violations; from there, he contends that a company need only make "reasonable efforts" to *try* to comply. Opp. 17-18; *see* Ex. 6 at 32 ("[S]omeone who wants to take biometric [data without consent] can do it as long as they act reasonably."). Next, he notes that BIPA permits an entity to obtain informed consent from a person or his "legally authorized representative." Opp. 17; 740 ILCS 14/15(b). He then asserts that Facebook could ask users to represent that *they* have received consent from any non-users (including strangers) who appear in their photos, as several other companies do. Opp. 18-19. He admits that Facebook would inevitably end up applying its technology to numerous non-users who did not provide the user with permission to consent on their behalf, but he asserts that Facebook would be shielded from liability because its conduct would not be negligent. Opp. 8.

The basic premise of Mr. Zellmer's argument is erroneous. Although Mr. Zellmer correctly points out that Facebook cannot be held liable for *damages* unless he carries his burden of proving at least negligence (740 ILCS 14/20(1)-(2)), neither *liability* nor the availability of BIPA's private right of action depends on a defendant's scienter. BIPA provides that "[a]ny person aggrieved by a violation" has a "right of action" and may pursue injunctive relief, various forms of monetary relief, and "other relief . . . as the State or federal court may deem appropriate." 740 ILCS 14/20(3)-(4). As Mr. Zellmer acknowledges (Opp. 8-9), the Illinois Supreme Court has made clear that a person is "aggrieved" by a violation *whenever* "a private entity fails to comply with one of [BIPA's notice-and-consent] requirements." *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 33 (2019). Because Facebook could not *possibly* comply with those requirements as to all non-users who appear in uploaded photos, Facebook would face potential liability under Mr. Zellmer's interpretation of BIPA even if it adopted the measures he proposes.

Mr. Zellmer's reading of BIPA would therefore effectively ban Facebook's technology, along with many other biometric systems. Mr. Zellmer does not dispute that the legislature intended to *promote* rather than *proscribe* such systems. *Compare* MSJ 19 *with* Opp. 17-20. But he fails to reckon with the implications of his claims. Facebook offered a hypothetical to illustrate this point: An industrial plant uses a biometric security system to verify the identities of individuals authorized to enter; an unauthorized entrant attempts to enter, has his face scanned, and is denied entry after the system finds no match and discards his data. MSJ 19-20. Under Mr. Zellmer's reading of BIPA, the company would be liable to the would-be intruder even though it did not know him and could not obtain his consent. Mr. Zellmer responds by assuming that the person would have committed a "criminal trespass" before being scanned and would therefore be barred by BIPA's negligence requirement from recovering. Opp. 19-20.

Again, the absence of negligence is not a complete defense to liability under BIPA. But in any event, there are many scenarios that do not involve a criminal trespass. Consider an iPhone owner who has enrolled in facial recognition for purposes of unlocking the device.[10] He leaves his phone on a park bench, and a stranger picks it up and looks at it, hoping to identify the owner so the device can be returned. The stranger's face is scanned and the device does not unlock. Under Mr. Zellmer's reading, Apple would be liable to the Good Samaritan.

To be clear, Facebook is not suggesting that the legislature intended to permit a company to *enroll* strangers in a biometric-identification system simply because it could not obtain their consent. And that is why Facebook does not create and store *templates* for non-users. Facebook's point is that for a biometric-identification system to function for *consenting users*, it must determine whether someone *is* one of those consenting users. This may require incidentally analyzing non-users to determine that there is no match. The legislature could not have intended for BIPA to apply to the ephemeral data, like non-user face signatures, created as part of that process—at least where, as here, obtaining consent would be impossible. *See People v. Russell*, 2012 Ill. App. 2d 111098-U, ¶ 15 (2012) ("our task is to effectuate the obvious intent of the General

[10] *Use Face ID on your iPhone or iPad Pro*, https://support.apple.com/en-us/HT208109.

Assembly" and "avoid[] the absurd result of punishing [defendants] where literal compliance with [the statute] is impossible"). The Court was correct in *Gullen*: Mr. Zellmer's case is not "what the BIPA was supposed to address." Ex. 6 at 34.

IV. MR. ZELLMER CANNOT OBTAIN AN INJUNCTION.

Even if the Court does not conclude that Facebook is entitled to summary judgment on the merits of Mr. Zellmer's claims, his brief confirms that his request for injunctive relief must be dismissed.

Injunctive relief is improper if "it isn't clear that all members of the class" would benefit from it, *Schulken v. Wash. Mut. Bank*, 2012 WL 28099, at *6 (N.D. Cal. Jan. 5, 2012), *or* if it would harm "individuals who are not members of the putative class[]," *Stokes v. CitiMortgage, Inc.*, 2015 WL 709201, at *10 (C.D. Cal. Jan. 16, 2015). As Facebook explained, Mr. Zellmer's requested injunction—"requiring Facebook to comply with the BIPA's requirements" as to non-users (Compl. ¶ 56)—would violate both of these principles. MSJ 20-21. Because obtaining consent from non-users is impossible, his proposed injunction would force Facebook to shut down facial recognition entirely. There is no evidence that even a substantial number of putative class members want that, and it is beyond dispute that many consenting Facebook *users* do not.

Mr. Zellmer again responds that complying with BIPA merely requires Facebook to show that it *tries* to obtain consent from non-users by asking users to obtain that consent on its behalf. Opp. 21. As discussed above, this argument is wrong as a matter of law. Mr. Zellmer has no serious defense to his claim for injunctive relief.

CONCLUSION

The Court should grant summary judgment in favor of Facebook on all of plaintiff's claims. In the alternative, it should grant summary judgment on his claim for injunctive relief.

Dated: June 22, 2021

MAYER BROWN LLP

By: /s/ Lauren R. Goldman
Lauren R. Goldman (*pro hac vice*)
Michael Rayfield (*pro hac vice*)
1221 Avenue of the Americas
New York, NY 10016
(212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

Matthew D. Provance (*pro hac vice*)
71 Wacker Drive
Chicago, IL 60606
(312) 701-8598
mprovance@mayerbrown.com

COOLEY LLP

Michael G. Rhodes (116127)
Whitty Somvichian (194463)
101 California Street, 5th Floor
San Francisco, CA 94111
(415) 693-2000
rhodesmg@cooley.com
wsomvichian@cooley.com

Attorneys for Defendant Facebook, Inc.